

12/31/98  
jc598 U.S. PTO

Please type a plus sign (+) inside this box →

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. K35A0576

Total Pages

First Named Inventor or Application Identifier

CHRISTOPHER L. HAMLIN

Express Mail Label No.

EJ794463159US

### APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

- Fee Transmittal Form  
(Submit an original, and a duplicate for fee processing)
- Specification [Total Pages 12]
  - Descriptive title of the Invention
  - Cross References to Related Applications
  - Statement Regarding Fed sponsored R & D
  - Reference to Microfiche Appendix
  - Background of the Invention
  - Brief Summary of the Invention
  - Brief Description of the Drawings (if filed)
  - Detailed Description
  - Claim(s)
  - Abstract of the Disclosure
- Drawing(s) (35 USC 113) [Total Sheets 3]
  - X Formal      Informal
- Oath or Declaration [Total Pages 2]
  - a.  Newly executed (original or copy)
  - b.  Copy from a prior application (37 CFR 1.63(d))  
(for continuation/divisional with Box 17 completed)  
*[Note Box 5 below]*
    - i.  DELETION OF INVENTOR(S)  
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
- Incorporation By Reference (useable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

ADDRESS TO: Assistant Commissioner for Patents  
Box Patent Application  
Washington, DC 20231

6.  Microfiche Computer Program (Appendix)
7. Nucleotide and/or Amino Acid Sequence Submission  
(if applicable, all necessary)
  - a.  Computer Readable Copy
  - b.  Paper Copy (identical to computer copy)
  - c.  Statement verifying identity of above copies

### ACCOMPANYING APPLICATION PARTS

8.  Assignment Papers (cover sheet & document(s))
9.  37 CFR 3.73(b) Statement  
(when there is an assignee)  Power of Attorney
10.  English Translation Document (if applicable)
11.  Information Disclosure Statement (IDS)/PTO-1449 [5] Copies of IDS Citations
12.  Preliminary Amendment
13.  Return Receipt Postcard (MPEP 503)  
(Should be specifically itemized)
14.  Small Entity  Statement filed in prior application, Statement(s)  Status still proper and desired
15.  Certified Copy of Priority Document(s)  
(if foreign priority is claimed)
16.  Other: Bibliographic Data  
.....  
.....

### 17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:

Continuation     Divisional     Continuation-in-part (CIP)    of prior application No: \_\_\_\_\_ / \_\_\_\_\_

### 18. CORRESPONDENCE ADDRESS

Customer Number or Bar Code Label  
(Insert Customer No. or Attach bar code label here) or  Correspondence address below

NAME	WESTERN DIGITAL CORPORATION				
	Milad G. Shara, Esq. - Reg. 39,367				
ADDRESS	8105 IRVINE CENTER DRIVE				
	PLAZA 3				
CITY	IRVINE	STATE	CALIFORNIA	ZIP CODE	92618
COUNTRY	U.S.A.	TELEPHONE	(949) 932-5676	FAX	(949) 932-5633

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

## Inventor Information

Inventor One Given Name :: Christopher L.  
Family Name :: Hamlin  
Name Suffix ::  
Postal Address Line One :: 310 Jensen Springs Rd  
City :: Los Gatos  
State/Province :: CA  
Country :: USA  
Postal or Zip Code :: 95030  
City of Residence :: Los Gatos  
Citizenship :: USA

## Correspondence Information

Name Line One :: Milad G. Shara, Esq.  
Name Line Two :: Western Digital Corporation  
Address Line One :: Plaza 3  
Address Line Two :: 8105 Irvine Center Drive  
City :: Irvine  
State/Province :: California  
Country :: USA  
Postal or Zip Code :: 92618  
Telephone :: (949) 932-5676  
Fax :: (949) 932-5633  
E-Mail :: Milad.G.Shara@wdc.com

## Application Information

Title Line One :: INTEGRATED CIRCUIT COMPRISING ENCRYPTION CIRCUITRY  
Title Line Two:: SELECTIVELY ENABLED BY VERIFYING A DEVICE  
Formal Drawings :: Yes  
Application Type :: Utility  
Docket Number :: K35A0576  
Licensed - U S Government Agency :: N/A  
Contract Number :: N/A  
Grant Number :: N/A  
Secrecy Order in Parent Application :: N/A

## Representative Information

Representative Customer Number :: Milad G. Shara, Esq.  
Registration Number One :: 39,367

1   **INTEGRATED CIRCUIT COMPRISING ENCRYPTION CIRCUITRY SELECTIVELY**  
2                   **ENABLED BY VERIFYING A DEVICE**  
3

4   **BACKGROUND OF THE INVENTION**

5   **Field of the Invention**

6         The present invention relates to encryption circuitry. More particularly, the present  
7   invention relates to an integrated circuit comprising encryption circuitry selectively enabled by  
8   verifying a device.

9   **Description of the Prior Art**

10        Cryptosystems are typically secure as long as attackers cannot discover the secret keys  
11   used to encrypt and decrypt messages. Attackers use various cryptanalysis techniques to analyze  
12   a cryptosystem in an attempt to discover the secret keys, where the difficulty in discovering the  
13   secret keys generally depends on the amount of information available. The cryptosystem typically  
14   employs a public encryption algorithm (such as RSA, DES, etc.), therefore an attacker typically  
15   knows the encryption algorithm and has access to ciphertext (encrypted text). However, it is  
16   usually very difficult to discover the secret keys with this information alone because an attacker  
17   typically needs to perform various operations on the ciphertext with respect to the original  
18   plaintext (unencrypted text). A known cryptanalysis technique includes monitoring a cryptosystem  
19   to capture plaintext before it is encrypted so that it can be analyzed together with the ciphertext.  
20   Another cryptanalysis technique includes performing a chosen plaintext attack by choosing the  
21   plaintext that is to be encrypted so as to expose vulnerabilities of a cryptosystem because the  
22   attacker can deliberately pick patterns helpful to analysis contributing to discovering the secret  
23   keys. This type of an attack can be defended against by requiring the individual clients accessing  
24   the cryptosystem to be authenticated. However, an attacker with direct access to a cryptosystem  
25   may attempt to circumvent such a requirement by tampering with the cryptosystem. Examples of  
26   tampering include inspecting, altering or replacing a component of the cryptosystem in order to  
27   force the encryption operation.

28        U.S. patent number 5,374,819 (the '819 patent) discloses a software program executing  
29   on a CPU which provides system operation validation in order to prevent the software program  
30   from executing on unlicensed computer systems. The validation method requires reading a unique  
31   chip identifier (chip ID) stored in a system device, and a corresponding chip ID and an encrypted

1 code stored in a non-volatile memory. The encrypted code, termed a message authentication  
2 code or MAC, is generated based on the chip ID using a secret key. The '819 patent relies on  
3 uncompromised secrecy of the secret key to prevent tampering which could circumvent the  
4 validation process.

5 The '819 patent is susceptible to a probing attacker attempting to discover the secret key  
6 by performing a chosen plain-text attack. For example, a probing attacker could tamper with the  
7 cryptosystem to generate chosen plaintext by modifying the chip ID stored in the non-volatile  
8 memory and then evaluate the resulting MAC generated by the encryption process. Further, a  
9 probing attacker could monitor the software program as it executes on the CPU in order to  
10 observe how the chosen plaintext is being encrypted using the secret key. If the secret key is  
11 discovered, the security of the system is compromised since the chip ID and corresponding MAC  
12 could be altered without detection.

13 There is, therefore, a need for a tamper resistant cryptosystem which is protected from an  
14 attacker employing chosen plaintext attacks.

## 15 SUMMARY OF THE INVENTION

16 The present invention may be regarded as an integrated circuit for selectively encrypting  
17 plaintext data received from a first device to produce encrypted data to send to a second device.  
18 The integrated circuit comprises controllable encryption circuitry comprising a data input, an  
19 enable input, and a data output. The integrated circuit further comprises a plaintext input for  
20 providing the plaintext data to the data input, an encrypted text output for providing the  
21 encrypted data from the data output, and a first control input for receiving a first device  
22 authentication signal for authenticating the first device. The integrated circuit further comprises a  
23 verification circuit responsive to the first device authentication signal for producing a first  
24 verification signal for use in controlling the enable input of the encryption circuitry to enable the  
25 encryption circuitry to provide the encrypted data via the encrypted text output.

26 The present invention may also be regarded as a method of controlling encryption circuitry  
27 within an integrated circuit by selectively encrypting plaintext data received from a first device to  
28 produce encrypted data to send to a second device. The method comprises the steps of receiving  
29 the plaintext data from the first device, receiving a first device authentication signal for  
30 authenticating the first device, producing a first verification signal in response to the first device

1 authentication signal, enabling the encryption circuitry in response to the first verification signal to  
2 provide the encrypted data to the second device.

### **3 BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 shows an embodiment of the present invention comprising a first device for providing plaintext data to an integrated circuit comprising an encryption circuit selectively enabled by a first device authentication signal generated by the first device, and a second device for receiving the encrypted data from the integrated circuit.

8 FIG. 2A shows a flow diagram for an embodiment of the present invention wherein an  
9 encryption operation is enabled by verifying a first device.

10 FIG. 2B shows a flow diagram for an alternative embodiment of the present invention  
11 wherein the encryption operation is enabled by verifying the first device  
12 and by verifying a second device, wherein the encrypted data is generated and sent to the second  
13 device only if both devices are verified.

## **DESCRIPTION OF THE PREFERRED EMBODIMENTS**

## System Overview

FIG. 1 shows an embodiment of the present invention comprising an integrated circuit 100 for selectively encrypting plaintext data 102 received from a first device 104 to produce encrypted data 106 to send to a second device 108. The integrated circuit 100 comprises controllable encryption circuitry 110 comprising a data input 112, an enable input 114, and a data output 116. The integrated circuit 100 further comprises a plaintext input 118 for providing the plaintext data 102 to the data input 112, an encrypted text output 120 for providing the encrypted data 106 from the data output 116, and a first control input 122 for receiving a first device authentication signal 124 for authenticating the first device 104. A first verification circuit 130, responsive to the first device authentication signal 124, produces a first verification signal 132 for use in controlling the enable input 114 of the encryption circuitry 110 to enable the encryption circuitry 110 to provide the encrypted data 106 via the encrypted text output 120.

27 The encryption circuitry 110 in the integrated circuit 100 will not operate unless the first  
28 device 104 has been verified which protects against a probing attacker tampering with the first  
29 device 104 in an attempt to perform a chosen plaintext attack. Further, the first device 104 will  
30 preferably not generate the first device authentication signal 124 unless a command to encrypt  
31 data is received by an authenticated client. This protects against an unauthenticated attacker

1 attempting to observe the first device authentication signal 124. Additional protection against  
2 observation may be provided by concealing the first device authentication signal 124 to deter  
3 probing, or by detecting an attacker's probing by, for example, monitoring changes to the  
4 impedance of the first device authentication signal 124. In an alternative embodiment discussed  
5 below, a message authentication code (MAC) is employed to protect against a chosen plaintext  
6 attack in the event that an attacker is able to observe the first device authentication signal 124. In  
7 yet another embodiment, a means is provided to verify the validity of the firmware executed by  
8 the first device 104. For example, a CRC check code may be generated for the firmware during  
9 manufacturing which is then verified during operation before generating the first device  
10 authentication signal 124. This protects against a probing attacker who tampers with the  
11 executable code in an attempt to force the first device 104 to generate the first device  
12 authentication signal 124.

13 To provide further protection against a probing attacker, in one embodiment both the  
14 integrated circuit 100 and the first device 104 are implemented using tamper-resistant encryption  
15 circuitry. An example discussion of tamper-resistant encryption circuitry is provided in Tygar,  
16 J.D. and Yee, B.S., "Secure Coprocessors in Electronic Commerce Applications," Proceedings  
17 1995 USENIX Electronic Commerce Workshop, 1995, New York, which is incorporated herein  
18 by reference.

19 In another embodiment, the integrated circuit 100 comprises a second control input 126  
20 for receiving a second device authentication signal 128 for authenticating the second device 108,  
21 and a second verification circuit 134 responsive to the second device authentication signal 128 for  
22 producing a second verification signal 136. A gating circuit 138 responsive to the first and  
23 second verification signals 124 and 128 applies an enable signal 140 to the enable input 114 to  
24 cause the controllable encryption circuitry 110 to provide the encrypted data 106 via the  
25 encrypted text output 120. In this embodiment, the encryption circuitry 110 in the integrated  
26 circuit 100 will not operate unless both the first device 104 and the second device 108 have been  
27 verified.

28 In the embodiment of FIG. 1, a cryptosystem comprises first device 104, integrated circuit  
29 100, and second device 108, wherein the first device 104 comprises a signal processing circuit and  
30 the second device 108 comprises a non-volatile memory. For example, in one embodiment a disk  
31 drive comprises a signal processing circuit 104 (e.g., a disk control system), a disk 108, and an

1 integrated circuit 100 comprising encryption circuitry 110. The disk drive preferably comprises a  
2 head disk assembly (HDA) and a printed circuit board (PCB), where the integrated circuit 100 can  
3 be located within the HDA or on the PCB. The encryption circuitry 110 implements a suitable  
4 cipher, such as the well known symmetric Data Encryption Standard (DES) or the asymmetric  
5 Rivest-Shamir-Adleman (RSA) algorithm. The encryption circuitry 110 is preferably implemented  
6 using suitable hardware, such as a family of linear feedback shift registers (LFSR) and other  
7 digital logic. An example of a hardware implementation of encryption circuitry is provided by  
8 Hans Eberle in “A High-Speed DES Implementation for Network Applications,” Technical  
9 Report 90, DEC System Research Center, September 1992, the disclosure of which is herein  
10 incorporated by reference.

## Device Verification

The first device 104 in FIG. 1 can be verified by incorporating within the first device 104 a unique device identifier which is transferred to the integrated circuit 100 as the first device authentication signal 124 whenever a request is received from an authenticated client to encrypt plaintext 102. In one embodiment, the first verification circuit 130 within the integrated circuit 100 comprises a comparator for comparing the device identifier received over line 124 with a corresponding expected device identifier. A match verifies that the first device 104 is authenticated and the encryption circuit 110 is enabled. The expected device identifier may be hardwired into the integrated circuit 100 (including blowing fuses), or it may be stored in non-volatile memory (such as on a disk). According to another embodiment, the expected device identifier can be stored as an encrypted text in the first device 104 and decryption circuitry is employed for decrypting the encrypted text.

23 Verifying the first device 104 using a unique device identifier prevents an attacker from  
24 replacing the first device 104 with a foreign device, thereby protecting against chosen plaintext  
25 attacks using foreign devices. However, an attacker may attempt to inspect or alter the first  
26 device 104 directly in an attempt to force the encryption circuit 110 to encrypt chosen plaintext.  
27 To protect against this type of inspection or alteration, an alternate authentication technique may  
28 be employed. For example, as discussed below, the authentication technique can include  
29 monitoring variations in spectral characteristics to assist in detecting attempts to inspect or alter  
30 the encryption circuit 110 or the first device 104.

1        In an alternative embodiment, a message authentication code (MAC) implemented within  
2 the first device 104 and the integrated circuit 100 is employed for generating the first device  
3 authentication signal 124 to verify the first device 104. Any suitable technique for implementing  
4 the MAC may be employed, such as the well known DES implementation. In particular, the first  
5 device 104 comprises a first device secret key for generating an initial MAC over the plaintext  
6 102 to be encrypted by the encryption circuit 110. The initial MAC is transferred to the  
7 integrated circuit 100 as the first device authentication signal 124. The first verification circuit  
8 130 within the integrated circuit 100 generates a verification MAC over the plaintext 102 using an  
9 internal secret key corresponding to the secret key that was used by the first device 104 to  
10 generate the initial MAC. The first verification circuit 130 compares the initial MAC (first device  
11 authentication signal 124) to the verification MAC where a match verifies that the first device 104  
12 is authenticated. In this embodiment, the first device authentication signal 124 (i.e., the initial  
13 MAC) may be observable by an attacker, but the secret keys and operation of the encryption  
14 algorithm to generate the initial MAC are preferably inaccessible to observation. In this manner,  
15 the MAC can deter employing chosen plaintext attacks since the encryption key for generating the  
16 MAC over the chosen plaintext must be known in order to generate the first device authentication  
17 signal 124.

18       Referring again to FIG. 1, another embodiment for verifying the first device 104 is to  
19 measure certain spectral characteristics of the cryptosystem during manufacturing, wherein the  
20 initial spectral signature is stored in an inaccessible area of the integrated circuit 100. During  
21 operation, the first device 104 generates an operating spectral signature for the cryptosystem  
22 which is transferred to the integrated circuit 100 as the first device authentication signal 124. The  
23 operating spectral signature can be transferred as a unique device identifier or included as part of  
24 a MAC. The first verification circuit 130 compares the initial spectral signature generated during  
25 manufacturing to the operating spectral signature where a match verifies that the first device 104  
26 is authenticated. Attempts to inspect or alter the cryptosystem, including attempts to induce  
27 errors by heating or irradiating the cryptosystem, will induce detectable changes in the spectral  
28 signature which will disable the encryption circuitry 110.

#### 29                      State Machine Control

30        In one embodiment, the integrated circuit 100 comprises state machine circuitry for  
31 implementing the device verification used to enable the encryption circuitry 110. The state

1 machine circuitry operates according to the flow diagrams set forth in FIG. 2A and 2B. At step  
2 142 the state machine receives a command from an authenticated client to encrypt plaintext. At  
3 step 144 a branch is executed based on whether the first device 104 is verified. The device  
4 verification may be implemented, for example, as described above. If the first device 104 is  
5 verified at step 144, then at step 146 the encryption circuitry 110 is enabled by the gating circuit  
6 138 and the plaintext is encrypted. The resulting encrypted data is then transferred at step 148 to  
7 the second device 108. If the first device 104 is not verified at step 144, then the encryption  
8 circuitry 110 is not enabled. FIG. 2B shows a flow diagram similar to that of FIG. 2A with the  
9 additional step 150 of verifying the second device 108 before gating circuit 138 enables the  
10 encryption circuitry 110.

**WE CLAIM:**

- 1 1. An integrated circuit for selectively encrypting plaintext data received from a first device  
2 to produce encrypted data to send to a second device, the integrated circuit comprising:  
3 controllable encryption circuitry comprising:
  - 4 a data input;
  - 5 an enable input;
  - 6 a data output;  
7 a plaintext input for providing the plaintext data to the data input;  
8 an encrypted text output for providing the encrypted data from the data output;  
9 a first control input for receiving a first device authentication signal for  
10 authenticating the first device; and  
11 a first verification circuit, responsive to the first device authentication signal, for  
12 producing a first verification signal for use in controlling the enable input of  
13 the encryption circuitry to enable the encryption circuitry to provide the  
14 encrypted data via the encrypted text output.
- 1 2. The integrated circuit as recited in claim 1, further comprising:
  - 2 a second control input for receiving a second device authentication signal  
3 authenticating the second device;
  - 4 a second verification circuit responsive to the second device authentication signal  
5 for producing a second verification signal; and
  - 6 a gating circuit responsive to the first and second verification signals for applying  
7 an enable signal to the enable input to cause the controllable encryption  
8 circuitry to provide the encrypted data via the encrypted text output.
- 1 3. The integrated circuit as recited in claim 1, wherein:
  - 2 the first device authentication signal comprises a device identifier; and
  - 3 the first verification circuit verifies the first device by comparing the device  
4 identifier to a corresponding expected device identifier.

1    4. The integrated circuit as recited in claim 3, wherein the expected device identifier is  
2       hardwired into the integrated circuit.

1    5. The integrated circuit as recited in claim 3, wherein:  
2              the second device is a non-volatile memory; and  
3              the expected device identifier is stored on the non-volatile memory.

1    6. The integrated circuit as recited in claim 1, wherein:  
2              the first device authentication signal comprises a message authentication code  
3                   generated over the plaintext data using a device key; and  
4              the first verification circuit verifies the first device by verifying the message  
5                   authentication code using an internal key.

1    7. The integrated circuit as recited in claim 1, wherein:  
2              the first device is a signal processing circuit; and  
3              the second device is a non-volatile memory.

1       8. A method of controlling encryption circuitry within an integrated circuit by selectively  
2           encrypting plaintext data received from a first device to produce encrypted data to send to  
3           a second device, the method comprising the steps of:  
4                  receiving the plaintext data from the first device;  
5                  receiving a first device authentication signal for authenticating the first device;  
6                  producing a first verification signal in response to the first device authentication  
7                  signal; and  
8                  enabling the encryption circuitry in response to the first verification signal to  
9                  provide the encrypted data to the second device.

1       9. The method of controlling encryption circuitry as recited in claim 8, further comprising the  
2           steps of:  
3                  receiving a second device authentication signal authenticating the second device;  
4                  producing a second verification signal in response to the second device  
5                  authentication signal; and  
6                  enabling the encryption circuitry in response to the first and second verification  
7                  signals to provide the encrypted data to the second device.

1       10. The method of controlling encryption circuitry as recited in claim 8, wherein:  
2                  the first device authentication signal comprises a device identifier; and  
3                  the step of producing a first verification signal in response to the first device  
4                  authentication signal comprises the step of comparing the device identifier  
5                  to a corresponding expected device identifier.

1       11. The method of controlling encryption circuitry as recited in claim 10, wherein the  
2           expected device identifier is hardwired into an integrated circuit.

1       12. The method of controlling encryption circuitry as recited in claim 10, wherein:  
2                  the second device is a non-volatile memory; and  
3                  the expected device identifier is stored on the non-volatile memory.

1    13. The method of controlling encryption circuitry as recited in claim 8, wherein:

2                 the first device authentication signal comprises a message authentication code

3                 generated over the plaintext data using a device key; and

4                 the step of producing a first verification signal in response to the first device

5                 authentication signal comprises the step of verifying the message

6                 authentication code using an internal key.

1    14. The method of controlling encryption circuitry as recited in claim 8, wherein:

2                 the first device is a signal processing circuit; and

3                 the second device is a non-volatile memory.

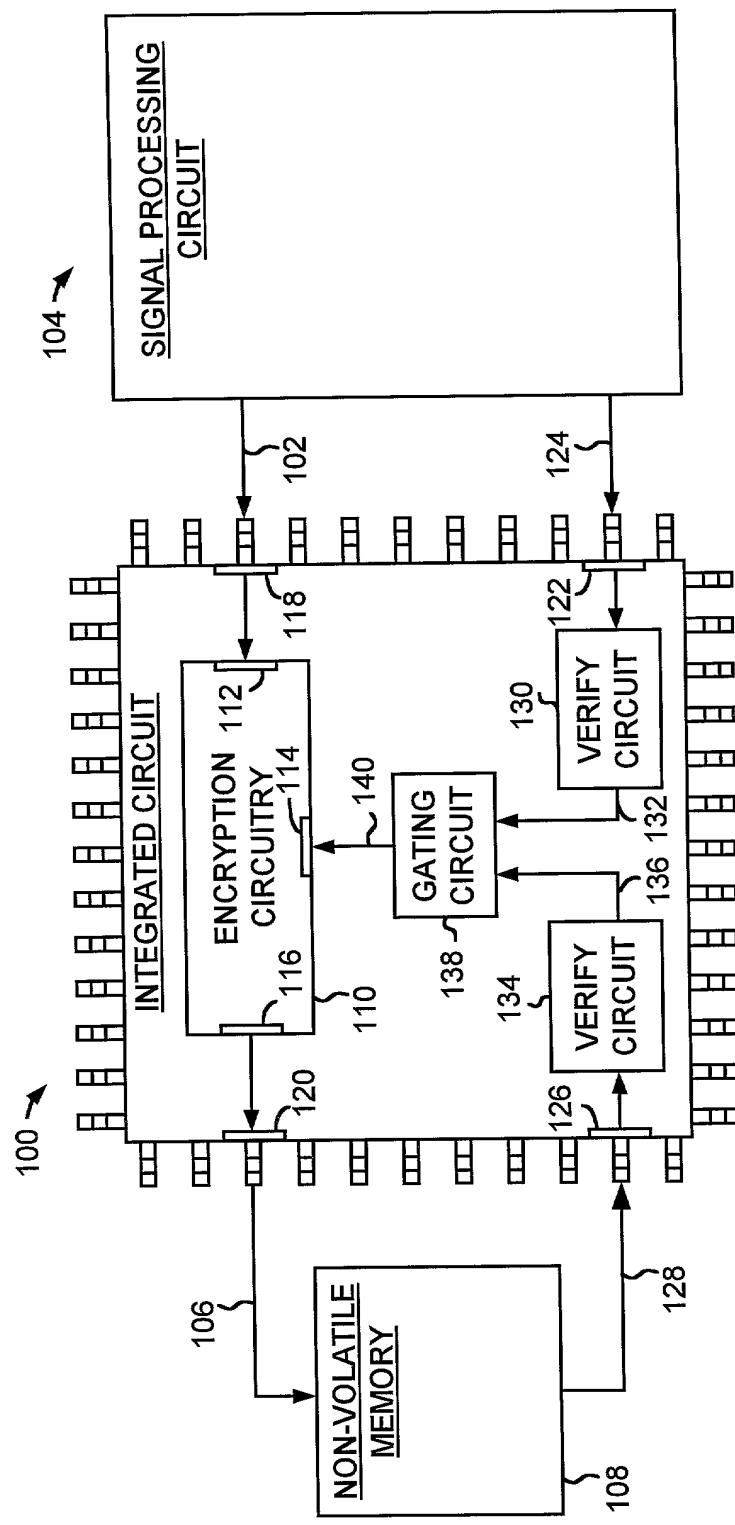
**1 INTEGRATED CIRCUIT COMPRISING ENCRYPTION CIRCUITRY SELECTIVELY**

**2 ENABLED BY VERIFYING A DEVICE**

3  
4

**5 ABSTRACT OF THE DISCLOSURE**

An integrated circuit is disclosed for selectively encrypting plaintext data received from a first device to produce encrypted data to send to a second device. The integrated circuit comprises controllable encryption circuitry comprising a data input, an enable input, and a data output. The integrated circuit further comprises a plaintext input for providing the plaintext data to the data input, an encrypted text output for providing the encrypted data from the data output, and a first control input for receiving a first device authentication signal for authenticating the first device. The integrated circuit further comprises a verification circuit responsive to the first device authentication signal for producing a first verification signal for use in controlling the enable input of the encryption circuitry to enable the encryption circuitry to provide the encrypted data via the encrypted text output.



**FIG. 1**

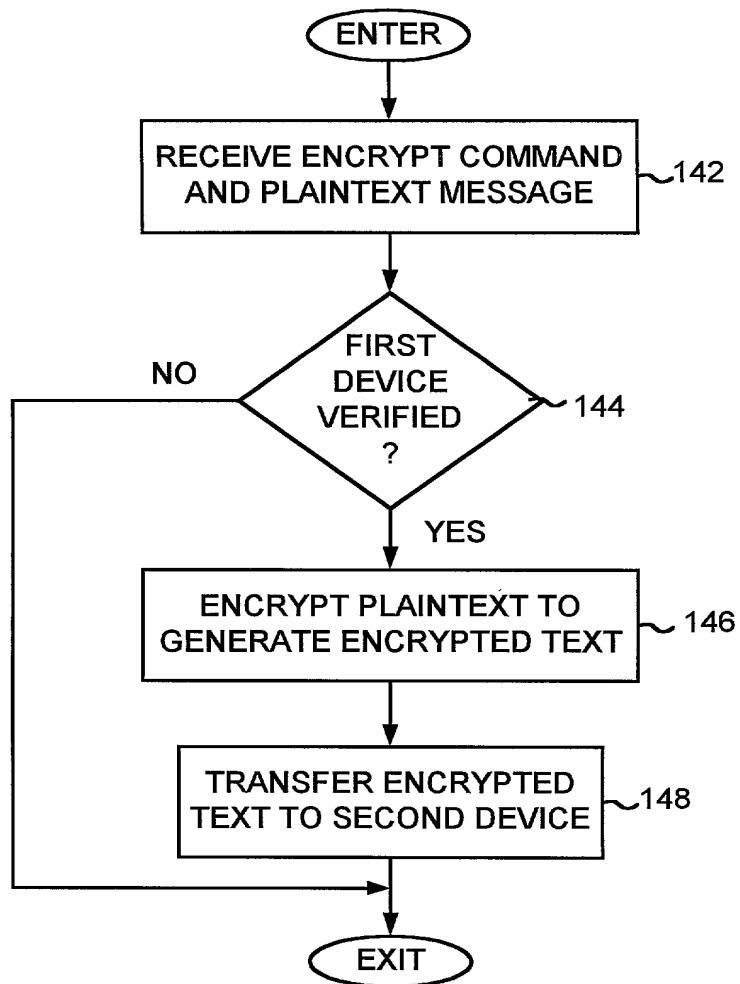


FIG. 2A

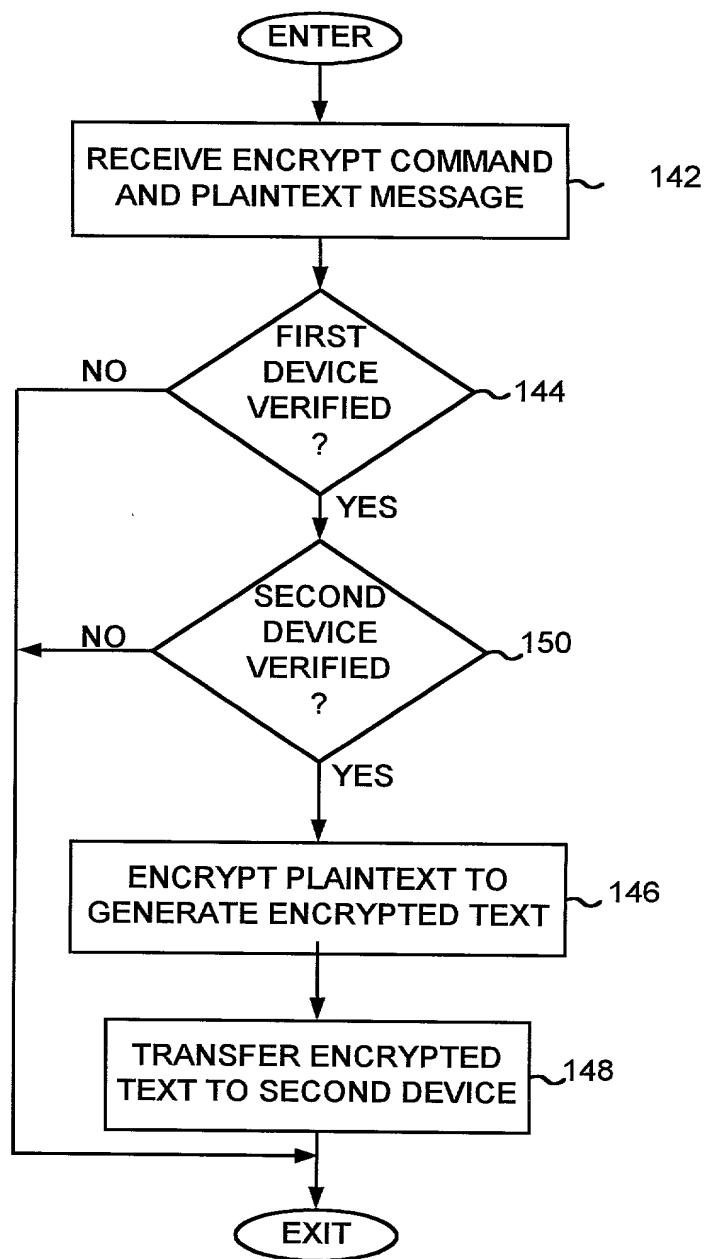


FIG. 2B

Please type a plus sign (+) inside this box → **[+]**

PTO/SB/01 (12-97)

Approved for use through 9/30/00 OMB 0651-0032

Patent and Trademark Office, U S DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

**DECLARATION FOR UTILITY OR  
DESIGN  
PATENT APPLICATION  
(37 CFR 1.63)**

Declaration Submitted with Initial Filing       Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

<b>Attorney Docket Number</b>		K35A0576
<b>First Named Inventor</b>		CHRISTOPHER L. HAMLIN
<b>COMPLETE IF KNOWN</b>		
Application Number		/ Unknown
Filing Date		Herewith
Group Art Unit		Unknown
Examiner Name		Unknown

**As a below named inventor, I hereby declare that:**

My residence, post office address, and citizenship are as stated below next to my name

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled.

**INTEGRATED CIRCUIT COMPRISING ENCRYPTION CIRCUITRY SELECTIVELY ENABLED BY VERIFYING A DEVICE**

the specification of which

*(Title of the Invention)*

is attached hereto  
OR

was filed on (MM/DD/YYYY)  as United States Application Number or PCT International

Application Number  and was amended on (MM/DD/YYYY)  (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES <input type="checkbox"/> NO <input type="checkbox"/>
			<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
			<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
			<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

Please type a plus sign (+) inside this box →

PTO/SB/01 (12-97)  
Approved for use through 9/30/00. OMB 0651-0032

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

## DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer Number  →  Registered practitioner(s) name/registration number listed below

Place Customer Number Bar Code Label here

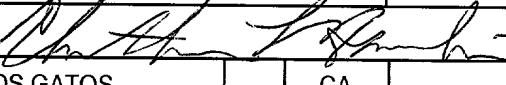
Name	Registration Number	Name	Registration Number
Milad G. Shara	39,367		

Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to:  Customer Number or Bar Code Label  OR  Correspondence address below

Name	Milad G. Shara		
Address	WESTERN DIGITAL CORPORATION		
Address	8105 Irvine Center Drive, Plaza 3		
City	Irvine	State	California
Country	U.S.A.	Telephone	(949) 932-5676
		ZIP	92618
		Fax	(949) 932-5633

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor:	<input type="checkbox"/> A petition has been filed for this unsigned inventor						
Given Name (first and middle if any)				Family Name or Surname			
CHRISTOPHER L.				HAMLIN			
Inventor's Signature						Date	12/22/99
Residence: City	LOS GATOS	State	CA	Country	USA	Citizenship	USA
Post Office Address	310 JENSEN SPRINGS RD						
Post Office Address							
City	LOS GATOS	State	CA	ZIP	95030	Country	USA
<input type="checkbox"/> Additional inventors are being named on the _____ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto							